

REMARKS

This amendment is responsive to the final Office Action¹ of February 8, 2005. Claims 1-37 were presented for examination. Claims 1, 13, 14 and 26 are independent claims and each has been amended herein. No new matter is added; support for the amendments is detailed below. No claims are canceled or added. Thus, claims 1-37 are pending.

All claims are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Further, all claims are rejected under 35 U.S.C. § 102(e) as being anticipated by Kung, U.S. Patent 5,241,594, (hereinafter "Kung"). Applicant respectfully traverses these rejections for the following reasons.

All claims (i.e., independent claims 1, 13, 14 and 26, and by dependency, claims 2-12, 15-25 and 27-37) are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. The Office Action indicates that the phrase "does not store" renders the claim indefinite, since computers inherently store all working data (Office Action, page 2). Applicant respectfully disagrees that the prior-submitted claims are indefinite, because "storing" information within the context of a computer environment normally means more than temporarily retaining working data in, e.g., a buffer or a register, for purposes of data manipulation or performing calculations, etc. Storing of data or information, in Applicant's

¹ The Office Action may contain a number of statements characterizing the cited references and/or the claims which Applicant(s) may not expressly identify herein. Regardless of whether or not any such statement is identified herein, Applicant(s) does not automatically subscribe to, or acquiesce in, any such statement. Further, silence with regard to rejection of a dependent claim, when such claim depends, directly or indirectly, from an independent claim which Applicant(s) deems allowable for reasons provided herein, is not acquiescence to such rejection of that dependent claim, but is recognition by Applicant(s) that such previously lodged rejection is moot based on remarks and/or amendments presented herein relative to that independent claim.

view, normally connotes relatively long-term retention of that data or information. Applicant's expression "does not store" was intended to be construed in this normal sense, and not in the extremely narrow sense seized-upon in the Office Action. That this was so intended is clear from Applicant's Remarks submitted in Applicant's previously filed response. "Since all authenticating information is erased or removed, it is clear that authenticating information is not stored in Applicant's server.....If the credentials cache is destroyed, then any information contained therein is likewise destroyed, wherefore it cannot be stored in the server." (Rule 111 Response, October 27, 2004, page 14) Clearly, a result of erasing information and destroying a cache is to not implement a storage function with respect to those items.

Nevertheless, rather than debate this point any further, to the potential delay in advancement of prosecution of this application, Applicant hereby amends all of its independent claims in a manner to avoid the alleged "indefiniteness". Applicant hereby deletes the language "does not store" and substitutes language regarding erasure of authenticating information and destruction of the credentials cache, as provided in the specification. In any event, it is respectfully submitted that the currently amended independent claims 1, 13, 14, and 26 and, by virtue of their respective dependencies, claims 2-12, 15-25 and 27-37 are not indefinite, wherefore the rejection under 35 U.S.C. § 112 second paragraph should be withdrawn.

Claims 1-37 are also rejected under 35 U.S.C. § 102(e) as being anticipated by Kung. However, Applicant's currently amended claims are not disclosed or suggested by Kung. Applicant's currently amended claim 1, for example, recites:

A method for providing secure communication of commands from a client to a plurality of hosts via a network server, comprising: utilizing authentication information and credentials cache information within the network server to facilitate the secure communication, wherein the authentication information is erased and the credentials

cache information is destroyed after the utilizing; receiving at least one command from the client; initiating one or more remote execution processes for processing the at least one command; transmitting the at least one command to one or more of the hosts via the one or more remote execution processes; obtaining, from the one or more remote execution processes, data associated with the one or more hosts executing the at least one command; formatting the data; and sending the formatted data to the client. (Emphasis added.)

By comparison, Kung discloses apparatus and methods for authenticating users in a distributed networked computing system (Abstract). Two embodiments are disclosed: a central server embodiment and a distributed system embodiment (Abstract). It is clear that Applicant's claimed subject matter includes a network server. If any portion of Kung may arguably be relevant to Applicant's claims, it would be Kung's central server embodiment portion. In Kung's central server embodiment a central server includes a file where ID's and encrypted passwords are stored (Abstract). Therein, all IDs and encrypted passwords are stored on a single computer (the server) that controls access to the entire distributed system. Once access is granted to a particular user, non-encrypted passwords are transmitted to the remote computers from the server, since the server controls the entire system (Abstract). This is further discussed in column 2, lines 16-21; column 2, lines 60-67; column 4, lines 24-25; column 4, lines 41-42 and elsewhere in Kung. Thus, it is clear that Kung stores its password and user ID information in its central server, precisely the opposite of what Applicant discloses and claims. Although Applicant's server utilizes authentication information and credentials cache information, the network server does not store that information because the authentication information is erased or removed and because the credentials cache is destroyed, as claimed.

Applicant's amendment is clearly supported by the application as originally filed. No new matter is added. For example, with respect to Applicant's Fig. 4, on page 24, lines 16-18,

the specification states: "The CGI Service Interface 740 then sends the encoded credentials cache information and a command form to web server 720, as indicated by arrow 760, destroys the credentials cache 830, then exits" (emphasis added). For another example, with respect to Fig. 6A, software processes CGI Service Interface 1000 and credentials cache 1080 are both included in Network Server 700 as shown. At the end of the discussion in the specification about the subject of issuing a command, referring to Figs. 6A/B and their related flowcharts Figs. 7A-7E, the following is stated: "CGI Service Interface 1000 destroys credentials cache 1080 and, then exits" (specification, page 30, line 13). Furthermore, support for erasing the authenticating information (client-authentication) is found in Applicant's specification with respect to Fig. 4:

The web server 720 encrypts the encoded credentials cache information and sends the data to the web browser 620, as well as a command form. Once the network server 700 sends the data to the client 600, all transient processes that handled the data exit and terminate and consequently, all authenticating information about client 600 is erased or removed. In order for client 600 to continue with the transaction, client 600 will have to refresh the memory of the server 720 and continue the second phase of the authentication process. Because there is no information relating to the transactions residing on the network server 700 during the time period in between transactions, if an unauthorized individual manages to improperly access the network server 700, as already explained above, any information obtained would be of limited value and the integrity of the system would be retained. (specification, page 25 lines 8-17, emphasis added).

Therefore, Applicant's specification/drawings teach, as exemplified above, that all authenticating information is erased or removed, wherefore it is clear that authenticating information is not stored in Applicant's server. Furthermore, since Applicant's specification/drawings teach, as exemplified above, that the credentials cache is destroyed, then any information contained therein is likewise destroyed and cannot be stored in the server. In other words, since the credentials cache is located in Applicant's server, and since no credential cache information can possibly remain in a credentials cache which has been destroyed, there plainly is no such information remaining or being stored in Applicant's server.

“Authentication information” and “credentials cache information”, or other terms that may be used synonymously for either type of information, or other terms that may be used to describe components of either type of information, are discussed throughout Applicant’s specification. In Applicant’s specification, for example, “credentials cache information” is discussed at least at: page 19, line 18; page 20, line 1; page 22, line 13; page 24, line 17; page 25, line 8; and “authenticating information” is discussed at least at page 25, line 11. These terms are thus defined in the specification and may be generally equivalent to the user ID’s and passwords of Kung. Accordingly, because Kung requires storage of its user ID’s and passwords in its central server but Applicant’s claim 1 recites language which prevents “authenticating information” and “credentials cache information” from being stored in Applicant’s network server, Applicant’s claim 1 clearly distinguishes over the Kung reference.

MPEP § 2131 indicates that to anticipate a claim, the reference must teach every element of the claim. In this instance, Kung does not teach every element of claim 1 since it does not teach, at least, “utilizing authentication information and credentials cache information within the network server to facilitate the secure communication, wherein the authentication information is erased and the credentials cache information is destroyed after the utilizing”, as claimed. Accordingly the 35 U.S.C. § 102(e) rejection of claim 1 should be withdrawn and the claim allowed. Claims 2-12 depend directly or indirectly from claim 1 and are allowable, at least for reasons based on their respective dependencies.

Independent claims 13 and 14 likewise recite, *inter alia*: “utilizing authentication information and credentials cache information within the network server to facilitate the secure communication, wherein the authentication information is erased and the credentials cache information is destroyed after the utilizing”, and are allowable for the same reasons as given

above for claim 1. Dependent claims 15-25 depend directly or indirectly from claim 14 and are allowable, at least for reasons based on their dependency.

Independent claim 26 recites, *interalia*: “A network server which utilizes authentication information and credentials cache information in transactions to facilitate secure communication, the network server being in communication with one or more clients and a plurality of hosts, the network server comprising: means for erasing the authentication information and for destroying the credentials cache information after each one of the transactions whereby the authentication information and credentials cache information are not stored in the server in-between the transactions”, and is allowable for the same reasons as given above. Support for this amendment is shown in the specification, page 25, lines 8-17, quoted above. Dependent claims 27-37 depend, directly or indirectly, from claim 26 and are allowable, at least for reasons based on their respective dependencies.

It is respectfully submitted that, as demonstrated above, the 35 U.S.C. § 102(e) rejection of all claims should be withdrawn and the claims allowed.

CONCLUSION

In view of the foregoing amendments and remarks, Applicant respectfully requests the reconsideration of this application and the timely allowance of the pending claims.

It is respectfully submitted that this amendment after final rejection should be entered since it does not change the scope of the claims - it merely presents the same scope in different phraseology for the purpose of overcoming the 35 U.S.C. § 112, second paragraph, rejection. This phraseology can be found in the specification as demonstrated. These amendments do not require the Examiner to do any further searching. Further, entry of this amendment shall narrow-down any contested issues that may be presented on appeal should the Examiner not be persuaded that these currently amended claims are patentable over the cited reference.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 07-2347 and please credit any excess fees to such deposit account. The Examiner is invited to telephone the undersigned at the telephone number provided below if he feels that a telephone conversation may serve to advance the prosecution of this application.

Verizon Corporate Services Group Inc.

By: 

Joel Wall
Reg. No. 25,648

Date: April 5, 2005
Verizon Corporate Services Group Inc.
C/O Christian Andersen
600 Hidden Ridge, HQE03H14
Irving, Texas 75038
(972) 718-4800

Customer No. 32127